PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference P034783-P0	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/JP2004/010068	International filing date *(day/month/year)* 08 July 2004 (08.07.2004)	Priority date *(day/month/year)* 08 July 2003 (08.07.2003)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 9 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 09 January 2006 (09.01.2006)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Masashi Honda
Facsimile No. +41 22 740 14 35	Telephone No. +41 22 338 70 10

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

REC'D 11 MAR 2005
WIPO PCT

From the
INTERNATIONAL SEARCHING AUTHORITY

PCT

To:

see form PCT/ISA/220

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

	Date of mailing *(day/month/year)* see form PCT/ISA/210 (second sheet)
Applicant's or agent's file reference see form PCT/ISA/220	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/JP2004/010068	08.07.2004	08.07.2003

International Patent Classification (IPC) or both national classification and IPC
G06F1/00, H04L9/32

Applicant
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA"). However, this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of three months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:

European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized Officer

Mäenpää, J

Telephone No. +49 89 2399-7287

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   ☐ This opinion has been established on the basis of a translation from the original language into the following language , which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23 1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

   ☐ a sequence listing

   ☐ table(s) related to the sequence listing

   b. format of material:

   ☐ in written format

   ☐ in computer readable form

   c. time of filing/furnishing:

   ☐ contained in the international application as filed.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	2-14,16-29,31-45,47-48,51,54,56-61
	No:	Claims	1,15,30,46, 49-50, 52-53, 55
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-61
Industrial applicability (IA)	Yes:	Claims	1-61
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Reference is made to the following documents:

D1: US-A-5 903 651 (KOCHER ET AL) 11 May 1999 (1999-05-11)
D2: XP001003705
D3: KOCHER P C: "ON CERTIFICATE REVOCATION AND VALIDATION" FINANCIAL CRYPTOGRAPHY. INTERNATIONAL CONFERENCE, XX, XX, 1998, pages 172-177, XP000997209

2 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of independent claims 1, 15, 30, 46, 49, 52, and 55 is not new in the sense of Article 33(2) PCT. The document D1 discloses the subject matter of claim 1 as follows (the references in parentheses applying to this document):

- information input/output system comprising (column 11, lines 18-13, "communication of medical records")
- an input/output device (figure 15: 1505 CERTIFICATE ACCEPTOR; column 10, lines 21-53)
- an information usage device (figure 15: 1504, CERTIFICATE HOLDER) that performs information input/output via the input/output device (column 11, lines 18-13, "communication of medical records")
- wherein the input/output device has the information usage device perform part of processing for judging whether the information usage device is one of valid and revoked (column 11, lines 18-13, "... parties holding digital certificates can obtain tree leaves corresponding to their own certificates and supply the tree and corresponding signature information along with the certificate. This eliminates the need for certificate recipients to independently download a CRL ...; column 10, lines 33-36")

The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent claims 15, 30, and 55, which therefore are also considered not new.

2.1 The document D1 discloses the following method steps and corresponding

executing features according to the features of claim 46 (the references in parentheses applying to this document):

- a list generation device for generation an identifier list that includes one or more identifiers corresponding to one or more valid or revoked devices (figure 15, tree issuer 1501; column 10, lines 21-28; figures 4-10; column 4, line 5 - column 8, line 26)

- a list storage unit (column 6, lines 43-46; column 8, lines 16-18, steps 1-3 include implicitly such a list storage unit)

- an acquiring unit operable to acquire on or more identifiers (column 10, lines 23-25)

- a generating unit operable to arrange the acquired identifiers according to a predetermined rule to generate an identifier list that includes the arranged identifiers (column 8, lines 16-18, steps 1-3) , and to write the generated identifier list to the list storage unit (column 8, steps 4 and 5 include implicitly such a writing step)

The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent claims 49 and 52, which therefore are also considered not new.

3 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claims 56-61 does not involve an inventive step in the sense of Article 33(3) PCT.

The document D1 is regarded as being the closest prior art to the subject-matter of claim 56, and discloses (the references in parentheses applying to this document):

- a judging method used in an input/output device (figure 15: CERTIFICATE ACCEPTOR 1505) via which an information usage device (figure 15: CERTIFICATE HOLDER 1504) performs information input/output (abstract, column 11, lines 18-13, "communication of medical records")

- receiving range information from the information usage device (column 10, lines 31-36), the range information showing a target range, specified using the identifier list, that includes a *target identifier* corresponding to the information usage device (figure 11,

step 1104; column 8, lines 41-46, "a leaf node representative of the *candidate item*")

NOTE: in D1 the information usage device (figure 15: CERTIFICATE HOLDER 1504) forwards the range information that it received from a confirmation issuer to the information input/output device.

- using the received range information in judging whether the information usage device is one of valid and revoked (figure 15: CERTIFICATE ACCEPTOR 1505; column 10, lines 33-36)

The subject-matter of the present claim 56 differs from D1 in that in the claim the the identifier list is outputted from the information input/output device to the information usage device that specifies the target range from it. In D1 the identifier list is outputted from a tree issuer to a confirmation issuer that searches the target range from it (column 8, lines 14-26, "publish the hash three and signed root node", "treeless variant in which individual ranges are signed directly"; figure 6; figure 10) (figure 15: TREE ISSUER 1501; figure 11, step 1101, "obtains the interval hash three") (figure 11, step 1104; column 8, lines 41-46, "a leaf node representative of the candidate item"). In D1 the confirmation issuer then issues that target range information to the information usage device (figure 11: step 1107) that further forwards this information to the information input/output device (column 10, lines 33-36). In D1 the information input/output device (figure 15: CERTIFICATE ACCEPTER 1505) is not involved in delivering the identifier list.

The technical problem solved by the difference to reduce the amount of physical entities in a validation system.

Combining separate logical functionalities residing in separate physical entities into a single entity is an obvious design option for the skilled person in order to achieve a system with lesser amount of entities.

The problem to be solved is an indication for the skilled person to combine the functionality of a confirmation issuer and a certificate holder (arriving at the information usage device of claim 56), and the functionality of the tree issuer and the certificate acceptor (arriving at the information input/output device of claim 56) and thereby arriving at a method of claim 56. See figure 15 of D1.

The above passages have been given in relation to the hash tree embodiment of D1. It should be noted that a similar argumentation is also possible starting from the "treeless" embodiment of D1 (figure 10), that specifies individually signed ranges as in the present application.

It should be noted that the solution enabling low processing power devices to validate other devices by avoiding long CRL searches in those devices is disclosed in D1 and the present application is relying on exactly the same solution: a confirmation issuer submitting self-verifying confirmations using signed ranges. The different distribution of the same logical functionalities in the present application does not make it inventive over D1.

The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent claims 57-61 which therefore are also considered not inventive.

4 Dependent claims 2-14, 16-29, 31-45, 47-48, 50-51 and 53-54 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of inventive step or novelty (claims 50 and 53), see documents D1 and D2 and the corresponding passages cited in the search report.

In particular the usage of lists of valid certificates instead of revoked certificates in claims 48, 51, and 54 is known in same context from D2.

The features of the other dependent claims are either obvious design options for the skilled person.

5 Additionally the present application does not meet the requirements of PCT in the following respects:

5.1 The computer programs and memory mediums (claims 57, 58, 60, 61) storing computer programs should be claimed by referring to the corresponding methods and not by repeating the wording of the corresponding method claims (Article 6 PCT).

5.2 The features of the claims are not provided with reference signs placed in

parentheses (Rule 6.2(b) PCT).

5.3 Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the documents D1 and D2 is not mentioned in the description, nor are these documents identified therein.